Square Pegs – Round Holes?

The History (and Future?) of e-Trespass

Scott M. Hervey
Weintraub Genshlea Chediak Sproul
400 Capitol Mall, 11th Floor
Sacramento, CA 95814
Telephone: 916-558-6000 Fax: 916-446-1611
shervey@weintraub.com www.weintraub.com

One who uses a chattel with the consent of another is subject to liability in trespass for any harm to the chattel which is caused by or occurs in the course of any use exceeding the consent, even though such use is not a conversion. Restatement (Second) of Torts, § 256 (1965)).

On December 10, 2001, in Intel Corporation v. Hamidi 94 Cal. App 4th 325 (2001), the California Court of Appeals upheld the trial court's issuance of an injunction preventing Kourosh Hamidi, a former employee of Intel Corporation, from sending unsolicited e-mail to addresses on Intel's computer system. Some commented that the decision was just the natural progression of the application of the law of trespass to disputes involving the Internet. However, on March 27, 2002, when the California Supreme Court granted cert, some began to question whether the Supreme Court would take this opportunity to reign in the application of trespass to chattels to Internet disputes.

Trespass and The Internet – The Early Years

Thrifty-Tel, Inc. v. Bezenek, 46 Cal.App.4th 1559 (1996) is the analytical starting point for all Internet trespass cases. In Thrifty-Tel the trial court entered judgment in

favor of a telephone long-distance carrier on fraud and conversion theories against the parents of teenage sons who cracked the phone company's access and authorization codes and made long distance phone calls without paying for them. On appeal, the defendants argued that the unauthorized use of the phone company's confidential codes for the purpose of gaining computer access did not constitute conversion. The tort provides a remedy for the loss of intangible property interest only if those interests are reflected in something tangible that can be physically taken.

At the time this case was decided the issue of whether computer code and the ting-up of Thrifty-Tel's system could be the subjects of conversion presented an issue of first impression. The appeal court found that even though the facts did not support a verdict of conversion as the property taken was intangible, the evidence supported a verdict of trespass to chattels.

The Internet in its Infancy

CompuServe Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D.Ohio,1997). CompuServe brought a trespass action against Cyber Promotions based on the numerous unsolicited e-mail advertisements it sent to CompuServe users. Prior to litigation, CompuServe notified the defendants that they were not allowed to use CompuServe computer equipment to process and store the unsolicited e-mail and requested that they terminate the practice. In response to CompuServe's request, the defendants sent an increasing volume of e-mail solicitations to CompuServe subscribers. CompuServe then attempted filter the spam, but the defendants were able to circumvent their efforts.

In this action CompuServe claimed that it received complaints from users threatening to discontinue their subscription unless CompuServe did something about the

spam. Because subscribers pay for their access to CompuServe's services in increments of time, the process of accessing, reviewing and discarding unsolicited e-mail was costing CompuServe users money, which was one of the reasons for their complaints. CompuServe also claimed that the volume of messages generated by the mass mailings places a significant burden on its equipment which has finite processing and storage capacity.

The court found that CompuServe, through its terms of service policy, expressly limited the consent it grants to Internet users to send e-mail to its proprietary computer systems by denying unauthorized parties the use of CompuServe equipment to send unsolicited electronic mail messages. The court found that Cyber Promotions used plaintiff's equipment in a fashion that exceeded that consent. Because the use of personal property exceeding consent is a trespass, the court found Cyber Promotions' conduct actionable.

America Online v. IMS, 24 F.Supp. 2d 548 (ED Virginia 1998). AOL brought an action against IMS on the grounds that its spam, among other things, violated Virginia's common law of trespass to chattel. The court found the facts of CompuServe nearly identical to the facts of the case at bar. In both cases, the defendants sent unsolicited e-mail advertising to hundreds of thousands of Internet users, many of whom were subscribers of the plaintiffs' Internet services; both defendants concealed the origin of their messages by forging header information; both plaintiffs alleged that processing the bulk e-mail cost them time and money and burdened their equipment; both plaintiffs contended that they received complaints from subscribers, and both contended that the

bulk e-mailers continued to send messages even after they were notified that bulk e-mailing was unauthorized.

The court heard evidence that the defendants intentionally sent over 60 million pieces of unsolicited bulk e-mail over a ten-month period. Further, the defendants admitted receiving a cease-and- desist letter from AOL and thereafter knew their contact with AOL's computer network was unauthorized, yet they continued spamming.

Because the court found the CompuServe so striking similar and the trespass law of Virginia so close to that of Ohio, the court noted its reliance on the reasoning of the CompuServe court and found trespass.

Hotmail Corp. v. Van Money Pie, Inc., 47 USPQ 2d 1020 (ND Cal 1998). In the Fall of 1997, Hotmail learned that the defendants were sending "spam" e-mails to thousands of Internet e-mail users, which falsely contained return addresses bearing Hotmail account return addresses when in fact such messages did not originate from Hotmail or a Hotmail account. These spam messages advertised pornography, bulk e-mailing software, and "get-rich- quick" schemes, among other things. Hotmail sought to enjoin the defendants through a number of claims, including a claim of trespass.

The court found that the evidence in the case supported a finding that Hotmail would prevail on its trespass to chattel claim. The court found that Hotmail had presented evidence that the computers, computer networks and computer services that comprise Hotmail's e-mail system are the personal property of Hotmail; that the defendants created Hotmail accounts pursuant to the limitations set forth in Hotmail's Terms of Service, that the defendants intentionally trespassed on Hotmail's property by knowingly and without authorization creating Hotmail accounts that were used for

purposes exceeding the limits of the Terms of Service; that the defendants trespassed on Hotmail's computer space by causing tens of thousands of misdirected e-mail messages to be transmitted to Hotmail without Hotmail's authorization, thereby filling up Hotmail's computer storage space and threatening to damage Hotmail's ability to service its legitimate customers; and that the defendants' acts of trespass damaged Hotmail in terms of added costs for personnel to sort through and respond to the misdirected e-mails, and in terms of harm to Hotmail's business reputation and goodwill.

America Online, Inc., v. LCGM, Inc., 49 F. Supp 2d 851 (E.D. Vir. 1999) was another of AOL's spam trespass case. AOL brought suit alleging that the defendants sent unauthorized and unsolicited bulk e-mail advertisements to AOL's customers. Like the cases before it, AOL claimed that the defendants intentionally used AOL's computers and computer network, which are tangible personal property, to send their spam to AOL users. And, like the cases before it, the court found that the undisputed facts established that the defendants' actions constituted a trespass to chattels under Virginia common law.

…Along Came a Spider

Prior to the turn of the century, the courts recognized that the transmission of unsolicited bulk e-mails can constitute a trespass to chattels. The year 2000 brought new technological advances, and claims of trespass resulting from their use.

In eBay, Inc. v. Bidder's Edge Inc. 100 F. Supp. 2d 1058 (N.D. Cal. 2000) the Northern District granted an injunction prohibiting Bidder's Edge from repeatedly accessing eBay's web site based on a theory of trespass to chattel under California law.

Bidder's Edge was an auction aggregation site designed to offer on-line auction buyers the ability to search for items across numerous on-line auctions without having to

search each site directly. Bidder's Edge provided these services through its use of a software robot (a computer program that operates across the Internet to perform searching, copying and retrieving functions on the web sites of others). Software robots are capable of executing thousands of instructions per minute; consume larger storage resources of the host system; and are capable of overloading the host system so as to cause it to crash.

In 1998, eBay gave Bidder's Edge permission to search its database for information regarding eBay hosted auctions for certain items. In early 1999, Bidder's Edge began to broaden the type of items for which it searched the eBay site. A dispute developed regarding the search method Bidder's Edge was to employ. The parties were not able to come to an agreement regarding the search method Bidder's Edge was to use, and in September 1999 eBay requested that Bidder's Edge stop posting eBay auction listings on its site. Bidder's Edge at first agreed, but later issued a press release that it would resume including eBay auction postings on its site.

eBay eventually filed a complaint and sought a preliminary injunction preventing Bidder's Edge from accessing the eBay system based on nine causes of action: trespass, false advertising, federal and state trademark dilution; computer fraud and abuse; unfair competition; misappropriation, interference with prospective economic advantage and unjust enrichment. In considering eBays motion, the court found that eBay had presented evidence of the possibility of suffering irreparable harm. eBay's allegation of harm was based, in part, on the argument that Bidder's Edge's activities should be thought of as equivalent to sending an army of 100,000 robots a day to check prices in a competitor's store. Further, eBay argued that if Bidder's Edge is allowed to continue unchecked, it

would encourage other auction aggregators to employ rude robots (robots that do not respect the Robot Exclusion Standard) to search the eBay system, thus causing irreparable harm from reduced system performance, system unavailability or date losses.

The court also found that eBay had established a likelihood of success under its claim for trespass to chattel. Although the court acknowledged that there is very little authority supporting a preliminary injunction based on an ongoing trespass to chattel, the court noted that "it is black letter law in California that an injunction is an appropriate remedy for a continuing trespass to real property." The court continued:

> if eBay were a brick and mortar auction house with limited seating capacity, eBay would appear to be entitled to reserve those seats for potential bidders, to refuse entrance to individuals (or robots) with no intention of bidding on any of the items, and to seek preliminary injunctive relief against non-customer trespasser eBay was physically unable to exclude. The analytical difficulty is that a wrongdoer can commit an ongoing trespass of a computer system that is more akin to the traditional notion of a trespass to real property, than the traditional notion of a trespass to chattel, because even thought it is ongoing, it will probably never amount to a conversion.

Bidder's Edge argued that it could not trespass eBay's web site because the site is publicly accessible. The court found this argument unconvincing since eBay's servers are "private property, conditional access to which eBay grants the public." eBay specifically precludes automated access. The court noted that in California, a trespass claim may lie where a defendant exceeds the scope of the license.

Register.Com, Inc., v. Verio, Inc., 126 F.Supp.2d 238 (SDNY 2000) pitted Internet domain name registrar against an Internet domain name registrar that provided website host services. The suit was the result of Verio's 1999 marketing campaign which specifically targeted customers in need of web hosting services. To reach those potential customers Verio developed an automated software program or "robot" that accessed the WHOIS database maintained by the accredited registrars, including Register.com, and collected the contact information of customers who had recently registered a domain name. Then, despite the marketing prohibitions in Register.com's terms of use, Verio utilized this data in its marketing to contact and solicit Register.com's customers.

The dispute centers on both Verio's end use of the WHOIS data and its use of the automated search robot. While Register.com acknowledged its obligation to provide public access to its customers' contact information, it claimed that its "terms of use" prohibits third parties, such as Verio, from using the contact information for any mass marketing purpose. Register.com also argued that Verio's use of an automated software robot to search the "WHOIS" database constituted trespass to chattels. Register.com stated that Verio's bots flooded its computer system with traffic in order to retrieve the contact information of Register.com customers for the purpose of solicitation in knowing violation of Register.com's posted policies and terms of use.

The court first found that Register.com's terms of use does not forbid the particular use of Viro's search robot. Register.com's posted policies and terms of use require a party who seeks access to its WHOIS database to agree that it will not "use this data to ... enable high volume, automated, electronic processes that apply to Register.com (or its systems)." The court found that the temporal aspect of this term only bars future

automated processes. Although Verio used an automated process to *collect* the WHOIS data, it does not then use the collected data to enable an automated process that applies to Register.com's systems. Once Verio's software robot secures the WHOIS information from Register.com's systems, it has completed its automated process with respect to Register.com's systems. The robot does not then use that WHOIS processes that apply to Register.com (or its systems)," it simply deposits the data into a database.

Despite the fact that Register.com's terms of use may not specifically forbid Verio's use of a search robot the court found that, at least the date the lawsuit was filed, Verio was made aware that Register.com does not consent to Verio's use of a search robot, and Verio is on notice that its search robot is unwelcome. The court warned that Verio's future use of a search robot to access the database exceeds the scope of Register.com's consent, and Verio would be liable for any harm to Register.com's computer systems.

Having established that Verio's access to its WHOIS database by robot was unauthorized, the court than reviewed Register.com's evidence that Verio's unauthorized access caused harm to its computer system. Although the court found Register.com's evidence of harm to its computer system caused by the successive queries performed by search robots lacking and imprecise, the evidence was enough to establish possessory interference which is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels.

The court found credible testimony that if the strain on Register.com's resources generated by Verio's searches becomes large enough, it could cause Register.com's computer systems to malfunction or crash. The court also reasoned that if Verio's

searching of Register.com's WHOIS database was determined to be lawful, then every purveyor of Internet-based services would engage in similar conduct. The court held that Register.com's evidence that Verio's search robots have presented and will continue to present an unwelcome interference with, and a risk of interruption to, its computer system and servers is sufficient to demonstrate a likelihood of success on the merits of its trespass to chattels claim.

And Back to Spam?

In Intel v. Hamidi, a former Intel employer who, after being terminated, launched a website <face-intel.com> for the purported purpose of providing a medium for Intel employees to air their questions and concerns over employment conditions at Intel. In the course of providing this open discourse for Intel employees, Hamidi also sent six e-mailings to between 8,000 and 35,000 employees through Intel's "internal, proprietary, email system." Only 450 requested to be removed from Hamidi's e-mail list.

Intel sent a letter to Hamidi requesting that he stop, but Hamidi refused. Intel also claimed that Hamidi took steps to evade technical measures instituted to prevent him from sending e-mail to Intel employees. According to Intel, its employees "spent significant amounts of time attempting to block and remove Hamidi's email from the Intel computer system."

Intel filed a complaint and sought relief based on the theory of trespass to chattels. The trial court granted Intel's motion for summary judgment and issued an injunction barring Hamidi from sending unsolicited e-mail to addresses on Intel's computer system. Hamidi appealed.

The majority of the court in Hamidi found that Intel had shown trespass to chattel. The court noted that a trespass to chattel is actionable *per se* without proof of actual damages; any authorized touching or moving of a channel is actionable even though no harm ensues. But to recover more nominal damages, the Plaintiff must show the value of the property taken or that he has sustained some special damages. As for Intel, the court noted that even assuming Intel had not demonstrated sufficient "harm" to trigger entitlement to nominal damages, it showed that Hamidi was disrupting its business by using its property, causing loss of productivity of thousands of employees distracted from their work, and had caused its security department to spend a good deal of time trying to stop the e-mails and therefore was entitled to injunctive relief based on the theory of trespass to chattel.

The dissenting opinion and amicus ACLU and Electronic Frontier Foundation raised interesting points with respect to the nature of the harm Intel allegedly suffered. While all acknowledged that common law doctrines evolve and adapt to new circumstances, they insisted that the foundational elements must remain the same. As for trespass to chattel, the dissenting opinion noted that Intel was still required to prove some injury to the chattel or at least to the possessory interest in the chattel. But, the only injury claimed by Intel, was the time spent by its employees reading a single e-mail. The dissent pointed out that the other decisions applying trespass to chattel with respect to the Internet have done so where the plaintiff has been able to prove that the transmittal of unsolicited bulk e-mail or the unauthorized search and retrieval of information from the plaintiff's database placed a burden on the computer system thereby reducing its capacity and slowing system performance. Both the dissenting opinion and amicus pointed out

that no case has yet to hold that reading an unsolicited message transmittal to a computer screen constitutes an injury that forms the basis for trespass to chattel.

Had Hamidi's conduct consisted of only sending six separate emails during the course of two years? The majority opinion clearly believed otherwise, noting that Hamidi, on six separate occasions, sent emails to between 8,000 and 35,000 Intel employees. Yet, the dissenting opinion argued that Intel was not dispossessed, even temporarily, of its e-mail system by reason of receipt of Hamidi's e-mail; the e-mail system was not impaired as to its condition, quality or value and no actual harm was caused to a person or thing in which Intel had a legally protected interest. The majority also suggests that injury to Intel resulted due to loss of productivity caused by the thousands of employees distracted from their work and by the time its security department spent trying to halt the incoming messages. However, as the dissenting opinion and amicus briefs note, the net effect was just one additional e-mail in a mail server inbox.

Where Are We Going

Trespass to chattel had been looked upon as the new panacea for parties on the receiving end of unwanted Internet conduct such as spamming, hacking, rude robots and spiders. Under such a claim, the plaintiff is entitled to an injunction without having to show injury, or complete loss of use of the chattel (database, server, etc). The party need only show that it was deprived of use of the chattel for a substantial time. The Supreme Court's decision in this case could have an impact on the use of the Internet and e-mail. If the court requires proof of a higher degree of injury then has been shown, e-Trespass may apply to only the most egregious violators and businesses may be required to rely on

technology to filter out the infrequent unwanted incoming spam, spiders or robots. However, if the court upholds the lower court's ruling, one may be able to claim that the time spent responding to allegedly trespassory conduct satisfies the tort's injury requirement, despite the fact that the value of the chattel or the user's ability to use the chattel remain unaffected.